Web Images Videos Maps News Shopping Gmail more ▼

Sign in

Google scholar braid group conjugacy problem Search

Advanced Scholar Search
Scholar Preferences

**Scholar** Articles and patents anytime include citations Results **1** - **10** of about **6,250**. (**0.09** sec)

A new approach to the word and **conjugacy problems** in the **braid** groups arxiv.org [PDF]

J Birman, KH Ko, SJ Lee - Advances in Mathematics, 1998 - Elsevier

**...** We also give a related solution to the **conjugacy problem**, but the improvements in its complexity are not clear at this writing. References. 1. SI Adjan, Defining relations and algorithmic **problems** for groups and semigroups. Proc. **...** 9. FA Garside, The **braid group** and other groups. **...**

Cited by 245 - Related articles - All 16 versions

The **braid group** and other groups

FA Garside - Quart. J. Math. Oxford, 1969 - Oxford Univ Press

**...** THE **braid group** B n+1 was first defined by Artin in a paper published in 1926 (1). The word **problem** for the **group** was solved **...** The primary concern will be to give the solution of the **conjugacy problem** in B n+1 . A new solution of the word **problem** is also given, and a new **...**

Cited by 396 - Related articles - All 3 versions

[PDF] An algebraic method for public-key cryptography psu.edu [PDF]

I Anshel, M Anshel, D Goldfeld - Mathematical Research Letters, 1999 - Citeseer

**...** An example is the **braid group** on n strands where the word **problem** for a word w (of length |w|) can be solved in running time O(|w| 2 n) while the best known algorithm for solving the **conjugacy problem** requires at least exponential running time (see [2]). Recent developments **...**

Cited by 191 - Related articles - View as HTML - BL Direct - All 11 versions

New key agreement protocols in **braid group** cryptography

I Anshel, M Anshel, B Fisher, D Goldfeld - Lecture Notes in Computer ..., 2001 - Springer

**...** was introduced for constructing key ag- reement protocols based on combinatorial **group** theory, the **...** security of the protocols was based on the difficulty of solving **conjugacy** and commutator **... Braid** groups provide a thread linking combinatorial **problems** in knot theory [10] to **...**

Cited by 63 - Related articles - BL Direct - All 4 versions

**Conjugacy problem** for **braid** groups and Garside groups arxiv.org [PDF]

N Franco, J Gonzalez-Meneses - Journal of Algebra, 2003 - Elsevier

**...** MathSciNet. [11]. FA Garside, The **braid group** and other groups. Quart. **...** Full Text via CrossRef. [13]. J. Michel, A note on words in **braid** monoids. J. Algebra 215 (1999), pp. **...** [15]. M. Picantin, The **conjugacy problem** in small Gaussian groups. Comm. Algebra 29 3 (2001), pp. **...**

Cited by 64 - Related articles - All 7 versions

A practical attack on some **braid group** based cryptographic primitives psu.edu [PDF]

D Hofheinz, R Steinwandt - Lecture notes in computer science, 2002 - Springer

**...** So we eventually obtain an algorithm for the **conjugacy problem** in the **braid group** B n : given v, w ∈ B n , we compute S(v) and one element w of S(w). Then v and w are **conjugate** iff w ∈ S(v). This approach cannot only be used to decide whether v and w are conjugated; it can **...**

Cited by 51 - Related articles - BL Direct - All 12 versions

New public-key cryptosystem using **braid** groups psu.edu [PDF]

KH Ko, SJ Lee, JH Cheon, JW Han, J Kang, C ... - Lecture Notes in ..., 2000 - Springer

**...** design. Key words: public key cryptosystem, **braid group**, **conjugacy problem**, key exchange, hard **problem**, non-commutative **group**, one-way function, public key infrastructure 1 Introduction 1.1 Background and Previous Results **...**

Cited by 184 - Related articles - BL Direct - All 18 versions

A POLYNOMIAL INVARIANT FOR KNOTS VIA VON NEUMANN ALGEBRAS1 mathaware.org [PDF]

VFR Jones - AMERICAN MATHEMATICAL SOCIETY, 1985 - ams.org

**...** union of the **braid** groups. Unforunately, although the **conjugacy problem** has been solved by F. Garside [8] within each **braid group**, there is no known algorithm to decide when (6, n) and (c, m) are equivalent. For a proof of **...**

Cited by 662 - Related articles - All 11 versions

The **conjugacy problem** in small Gaussian groups

M Picantin - Communications in Algebra, 2001 - Citeseer

**...** We show here how to extend the Elrifai-Morton solution for the **conjugacy problem** in **braid** groups to every small Gaussian **group**. **...** We show here how to extend the Elrifai-Morton solution for the **conjugacy problem** in **braid** groups to every small Gaussian **group**. Citations. **...**

Cited by 34 - Related articles - Cached - BL Direct - All 3 versions

A polynomial time algorithm for the **braid** Diffie-Hellman **conjugacy problem** psu.edu [PDF]

JH Cheon, B Jun - Advances in cryptology–CRYPTO, 2003 - Springer

**...** Keywords: **Braid group**, Non-abelian **group**, **Conjugacy Problem** 1 Introduction **...** Their basic mathematical **problem** is the **Conjugacy Problem** (CP) on **braids**: For a **braid group** B n , we are asked to find a **braid** a from u, b ∈ B n satisfying **...**

Cited by 39 - Related articles - All 16 versions

Gooooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next** braid group conjugacy problem Search

Go to Google Home - About Google - About Google Scholar